Section C - Descriptions and Specifications

STATEMENT OF WORK

**STATEMENT OF WORK**

**PROJECT TITLE:** Contractor support for the SAIL-ON program

## 1.0 PURPOSE

### 1.1 SCOPE

The purpose of this contractor is to provide contract support for the SAIL-ON program. This contract will be CPFF
level of effort contract, with one (1) five-month base period and one (1) one-year option period. Services provided are severable.

### 1.2 BACKGROUND

The Science of Artificial Intelligence and Learning for Open-world Novelty (SAIL-ON) program will research and develop the underlying scientific principles and general engineering techniques and algorithms needed to create AI systems that act appropriately and effectively in novel situations that occur in open worlds, which is a key characteristic needed for potential military applications of AI. The focus is on novelty that arises from violations of implicit or explicit assumptions in an agent's model of the external world, including other agents, the environment, and their interactions. Specifically, the program will:

(1) Develop scientific principles to quantify and characterize novelty in open world domains;

(2) Create AI systems that act appropriately and effectively in open world domains; and

(3) Demonstrate and evaluate these systems in multiple domains, including a selected DoD domain.

These three goals correspond to Technical Areas (TAs) 1, 2, and 3, respectively.

The TA3/Government team will facilitate and oversee evaluations of the TA2 technology against the TA1 novelty generators (SAIL-ON Task 3.1), identify DoD test domains and selection criteria (SAIL-ON Task 3.2), and augment TA1 and TA2 technologies to apply them to a DoD domain (SAIL-ON Tasks 3.3 a & b, respectively).

During Phase 2, TA3 will develop the capstone application allowing for experimentation with the TA1/TA2 developed technologies in a military domain. In particular, NIWC Pacific will work to generate novelty in experiments using TA1 approaches and employ TA2 approaches for detecting and responding to novelty using ONR Minerva applications.

SAIL-ON selected capstone domains include Minerva RTI simulation mission planning environment and live experimentation environment for the purposes of CUBRC contract.

## 2.0 APPLICABLE DOCUMENTS

DODI 5200.48, Controlled Unclassified Information (CUI), 6 March 2020

## 3.0 PERFORMANCE REQUIREMENTS

CUBRC SOW Tasks:

1. NOVELTY IN THE DOD DOMAIN (TA3.1 CUBRC): Support integration of novelty definitions within militarily relevant scenarios appropriate for the SAIL-ON Capstone DOD domain.

2. NOVELTY GENERATION/EXPERIMENT EXECUTION PIPLELINE (TA3.1 CUBRC): Support development software pipeline to drive and execute experimentation campaigns/battle scenarios with novelty injection.

    a. Demonstrate execution pipeline for preliminary experiments.
    b. Provide basic documentation/training to NIWC, allowing NIWC configuration and execution of novelty generation and experimentation pipeline.
    c. Continue to evolve pipeline to support higher levels of novelty for Phase III.

3. NOVELTY DATA ANALYTICS PIPLELINE (TA3.1 CUBRC): Support development data analytics pipeline to collect and analyze scenario campaign experiment data to generate SAIL-ON-style performance graphs (with and without novelties injected) and SAIL-ON program metrics.
    a. Provide basic documentation/training to NIWC, allowing NIWC configuration and execution of data analytics pipeline.
    b. Continue to evolve pipeline to support higher levels of novelty for Phase III.

4. DEVELOP PROTOTYPE (TA3.2 CUBRC): Support NIWC integration and development efforts of capstone agents, utilizing SAIL-ON TA2 performer solutions, into the DoD capstone domains for experimentation and demonstration efforts.

5. CONDUCT DEMONSTRATION OF NOVELTY EXPERIMENTS (TA3.1 CUBRC): Support execution of SAIL-ON capstone simulation evaluations, dry runs, simulated and/or live demonstrations as planned per SAIL-ON program schedule.

6. PLANS AND REPORTS: Support NIWC planning/report/powerpoint generation for briefings to DARPA SAIL-ON leadership for capstone monthly progress meetings, sail-on pi meetings, sail-on capstone planning meetings, sail-on capstone design reviews, capstone dry runs/demonstration/experimentation/evaluation; as needed.

**4.0 TRAVEL**

Travel will be contemplated during the post-award stage. No travel cost will be included in the cost proposal.

**5.0 PROPERTY REQUIREMENTS**

Not applicable

**6.0 SECURITY**

The contractor(s) are performing unclassified work and require access to government computers. Therefore, NIWC PAC Personnel Security is responsible for making a Fitness Determination in regards to CAC issuance. A CAC will be conditionally authorized provided the contractor meets the required benchmarks (i.e., favorable fingerprints, successfully submitted background investigation questionnaire, etc.).

6.1 Operations Security (OPSEC). OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

6.2.1 Operations Security (OPSEC) Requirements

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function, which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E SECNAVINST 3070.2A, and NAVWARINST 3432.1, NAVWAR/NIWC Atlantic/NIWC Pacific's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel have access to classified information, unclassified Critical Program Information (CPI), Controlled Unclassified Information (CUI) or Department of Navy (DoN) networks.

6.2.2 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the NAVWARINST 3432.1 and existing local site OPSEC procedures. The Contractor shall development their own internal OPSEC program specific to the contract and based on NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC requirements. The Contractor's program shall identify the current contractor site OPSEC Officer/Coordinator/POC.

6.2.3 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the government or by the contractor's OPSEC Manager. Contractor training shall include, at a minimum, cover OPSEC as it relates to contract work; discuss the Critical Information applicable in the contract; applicable review of government Critical Information and Indicators List(s) (CIIL); social media awareness and vulnerabilities; local threats; how to protect, transmit, and destroy controlled unclassified information; risks and guidance pertaining to geolocation-capable devices, applications, and services; and OPSEC review procedures for public release. The Contractor shall ensure that training materials developed by the Contractor shall be reviewed by the NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC Officer, who will ensure it is consistent with NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC policies. OPSEC training requirements are applicable for personnel during their entire term supporting NAVWAR/NIWC Atlantic/NIWC Pacific contracts and for the duration of DoN network access.

6.2.4 NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC Program

If required, the Contractor shall participate in NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC program briefings and working meetings, and complete any required OPSEC survey or data call within the timeframe specified.

6.3 Information Security

Pursuant to DoDM 5200.01 and DoDI 5200.48, the contractor shall provide adequate security for all CUI and Unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. If the contractor originates, adds to, or changes any of the DoD information, it must be marked in accordance with DODI 5200.48 and handled properly. The contractor shall disseminate CUI and unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

6.4 Contractor Requirements for Intelligence Oversight
In compliance with DoDD 5148.13 paragraph 4.1.e and SECNAVINST 3820.3F, all contractor personnel conducting Intelligence or Intelligence-related activities or supporting those efforts under Department of Defense authorities shall report any Questionable Intelligence Activity (QIA) or Significant or Highly Sensitive Matter (S/HSM) to the Naval Information Warfare Systems Command Intelligence Oversight Program Manager or Senior Intelligence Officer.

6.4.1 Questionable Intelligence Activity (QIA): Any Intelligence or Intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

6.4.2 Significant or Highly Sensitive Matter (S/HSM): An Intelligence or Intelligence-related activity (regardless of whether the Intelligence or Intelligence-related activity is unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by Intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of Intelligence activities. Such matters might involve actual or potential:

- Congressional inquiries or investigations.
- Adverse media coverage.
- Impact on foreign relations or foreign partners.
- Systemic compromise, loss, or unauthorized disclosure of protected information.

**7.0 DELIVERABLES**

See attached CDRLs.

**8.0 PERFORMANCE CRITERIA**
Not applicable.

SOW ADDENDUM

# NIWC Pacific PWS/SOW Addendum

## I. NIWC PACIFIC WORK WEEK

(a) All or a portion of the effort under this contract will be performed on a Government installation. The normal work week for Government employees at NIWC Pacific is Monday through Thursday 7:15 AM to 4:45 PM and Friday 7:15 AM to 3:45 PM with every other Friday a non-work day. Work at this Government installation, shall be performed by the contractor within the normal work hours at NIWC Pacific unless differing hours are specified on an individual delivery/task order. The contractor is not required to maintain the same hours as Government employees; however, contractor employees performing work at NIWC Pacific must work during the normal workweek. The following is a list of holidays observed by the Government.

| Name of Holiday | Time of Observance |
|---|---|

| | |
|---|---|
| New Year's Day | 1 January |
| Martin Luther King Jr. Day | Third Monday in January |
| Presidents Day | Third Monday in February |
| Memorial Day | Last Monday in May |
| Juneteenth National Independence Day | 19 June |
| Independence Day | 4 July |
| Labor Day | First Monday in September |
| Columbus Day | Second Monday in October |
| Veteran's Day | 11 November |
| Thanksgiving Day | Fourth Thursday in November |
| Christmas Day | 25 December |

(b) If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the contractor in accordance with the practice as observed by the assigned Government employees at the using activity.

(c) If the contractor is prevented from performance as the result of an Executive Order or an administrative leave determination applying to the using activity, such time may be charged to the contract as direct cost provided such charges are consistent with the contractor's accounting practices.

(d) This contract does not allow for payment of overtime during the normal workweek for employees who are not exempted from the Fair Labor Standards Act unless expressly authorized by the Ordering Officer. Under Federal regulations, the payment of overtime is required only when an employee works more than 40 hours during a week. Therefore, during the NIWC Pacific off-Friday (36-hour) week overtime will not be paid for non-exempt employees. During the work-Friday week (44 hour) the contractor is to schedule work so as not to incur overtime charges during the normal work week unless authorized in writing by the Government to do so. An example of this would be for contractor personnel to work during the hours of 7:15 AM to 4:45 PM Monday through Thursday and 7:15 AM to 3:45 PM Friday during the work-Friday week. The contractor may also elect to configure the workforce in such a way that no single employee exceeds 40 hours during a normal week even though normal NIWC Pacific hours are maintained both weeks.

(e) NOTICE: All contractor employees who make repeated deliveries to military installations shall obtain the required employee pass via the Defense Biometric Identification System (DBIDS) in order to gain access to the facility. Information about DBIDS may be found at the following website: https://www.cnic.navy.mil/om/dbids.html.

Contractor employees must be able to obtain a DBIDS in accordance with base security requirements. Each employee shall wear the Government issued DBIDS badge over the front of the outer clothing. When an employee leaves the contractor's employ, the employee's DBIDS

badge shall be returned to the Contracting Officer's Representative or the base Badge and Pass Office within five (5) calendar days.

Contractors who do not have a DBIDS or Common Access Card (CAC) must be issued a one-day pass daily at the Badge and Pass Office. Issuance of a CAC requires the need for physical access to the installation and logical access to government owned computer systems.

(f) Periodically, the Government may conduct Anti-Terrorism Force Protection (AT/FP) and/or safety security exercises, which may require the contractor to adjust its work schedule and/or place of performance to accommodate execution of the exercise. The contractor will be required to work with its Government point of contact to adjust work schedules and/or place of performance in the case of an exercise that causes disruption of normally scheduled work hours or disruption of access to a government facility. The contract does not allow for payment of work if schedules cannot be adjusted and/or the work cannot be executed remotely (i.e., the contractor's facility or alternate non-impacted location), during an exercise when government facilities are inaccessible.

## II. LIABILITY INSURANCE--COST TYPE CONTRACTS

(a) The following types of insurance are required in accordance with FAR 52.228-7 “Insurance--Liability to Third Persons” and shall be maintained in the minimum amounts shown:

(1) Workers’ compensation and employers’ liability: minimum of $100,000
(2) Comprehensive general liability: $500,000 per occurrence
(3) Automobile liability: $200,000 per person
$500,000 per occurrence
$ 20,000 per occurrence for property damage

(b) When requested by the contracting officer, the contractor shall furnish to the Contracting Officer a certificate or written statement of insurance. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness (i.e., performance period), and contract number. The contract number shall be cited on the certificate of insurance.

## III. KEY PERSONNEL

(a) The offeror agrees to assign to this contract those key personnel listed in paragraph (d) below. No substitutions shall be made except in accordance with this text.

(b) The offeror agrees that during the first 30 days of the contract performance period no personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death or termination of employment. In any of these events, the contractor shall promptly notify the Contracting Officer and provide the information required by paragraph (c) below. After the initial 30 day period, all proposed substitutions must be submitted in writing, at least fifteen (15) days (thirty (30) days if a security clearance is to be obtained) in advance of the proposed substitutions to the contracting officer. These substitution requests shall provide the information required by paragraph (c) below.

(c) All requests for approval of substitutions under this contract must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute or addition, and any other information requested by the Contracting Officer or needed by him to approve or disapprove the proposed substitutions. All substitutions proposed during the duration of this contract must have qualifications of the person being replaced. The Contracting Officer or authorized representative will evaluate such requests and promptly notify the contractor of approval or disapproval thereof in writing.

(d) List of Key Personnel

| NAME | CONTRACT LABOR CATEGORY |
|---|---|
| None | |
| | |
| | |

(e) If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the contract work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate. In addition, if the contractor is found at fault for the condition, the Contracting Officer may elect to equitably decrease the contract price or fixed fee to compensate the Government for any resultant delay, loss or damage.

(f) If the offeror wishes to add personnel to be used in a labor category, it shall employ the procedures outlined in paragraph (c) above. Adding personnel will only be permitted in the event of an indefinite quantity contract, where the Government has issued a delivery order for labor hours that would exceed a normal forty hour week if performed only by the number of employees originally proposed.

## IV. CONTRACTOR IDENTIFICATION

(a) Contractor employees must be clearly identifiable while on Government property by wearing appropriate badges.

(b) Contractor personnel and their subcontractors must identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract.

(c) Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles must be clearly identified with contractor supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

## V. REIMBURSEMENT OF TRAVEL COSTS

(a) Contractor Request and Government Approval of Travel

Any travel under this contract must be specifically requested in writing, by the contractor prior to incurring any travel costs. If this contract is an indefinite-delivery contract, then the written Government authorization will be by task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order. If this contract i an indefinite-delivery contract, then the written Government authorization will be by written notice of approval from the Contracting Officer's Representative (COR). The request shall, at a minimum, include:

(1) Contract number
(2) Date, time, and place of proposed travel
(3) Purpose of travel and how it relates to the contract
(4) Contractor's estimated cost of travel
(5) Name(s) of individual(s) traveling and;
(6) A breakdown of estimated travel and per diem charges.

(b) General

(1) The costs for travel, subsistence, and lodging shall be reimbursed to the contractor only to the extent that it is necessary and authorized for performance of the work under this contract. The costs for travel, subsistence, and lodging shall be reimbursed to the contractor in accordance with the Federal Acquisition Regulation (FAR) 31.7 Contracts with Nonprofit Organizations, the cost principles prescribed in 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements, which is incorporated by reference into this contract.

(2) Personnel in travel status from and to the contractor's place of business and designated work site or vice versa, shall be considered to be performing work under the contract, and contractor shall bill such travel time at the straight (regular) time rate; however, such billing shall not exceed eight hours per person for any one person while in travel status during one calendar day.

(c) Per Diem

(1) The contractor shall not be paid per diem for contractor personnel who reside in the metropolitan area in which the tasks are being performed. Per diem shall not be paid on services performed at contractor's home facility and at any facility required by the contract, or at any location within a radius of 50 miles from the contractor's home facility and any facility required by this contract.

(2) Costs for subsistence and lodging shall be paid to the contractor only to the extent that overnight stay is necessary and authorized in writing by the Government for performance of the work under this contract per paragraph (a). When authorized, per diem shall be paid by the contractor to its employees at a rate not to exceed the rate specified in the contractor's approved travel policy in accordance with FAR 31.7 Contracts with Nonprofit Organizations, the cost principles prescribed in 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements.

## VI. REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION

(a) Definition. As used in this text, "sensitive information" includes:

(i) All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;

(ii) Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC Ch. 21);

(iii) Information properly marked as "business confidential," "proprietary," "procurement sensitive," "source selection sensitive," or other similar markings;

(iv) Other information designated as sensitive by the Naval Information Warfare Systems Command (NAVWAR).

(b) In the performance of the contract, the contractor may receive or have access to information, including information in Government information systems and secure websites. Accessed information may include "sensitive information" or other information not previously made available to the public that would be competitively useful on current or future related procurements.
(c) Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The contractor shall—

(i) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;
(ii) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal statute, law, or regulation;
(iii) Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contact and to safeguard information from unauthorized use and disclosure.
(iv) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment;
(v) Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

(d) In the event that the contractor inadvertently accesses or receives any information marked as "proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the contractor may not be authorized to access such information, the contractor shall (i) notify the Contracting Officer; and (ii) refrain from any further access until authorized in writing by the Contracting Officer.

(e) The requirements of this text are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA) training certificate, SF85P, or other forms that may be required for access to Government information systems.

(f) Subcontracts. The contractor shall insert paragraphs (a) through (f) of this text in all subcontracts that may require access to sensitive information in the performance of the contract.

(g) Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the contractor's plan to implement the requirements of paragraph (c) above and shall include the use of a firewall to separate contractor personnel requiring access to information in the performance of the contract from other contractor personnel to ensure that the contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

## VII. DESIGNATION OF CONTRACTING OFFICER'S REPRESENTATIVE

The Contracting Officer hereby appoints the following individual as Contracting Officer's Representative (COR) for this contract/order:

Name: Rose Aubuchon
Code: 53608
Phone Number: (619) 553-1897
E-mail: rose.l.aubuchon.civ@us.navy.mil

## VIII. TECHNICAL DIRECTION

(a) Technical Direction may be provided to the contractor from time to time by the Contracting Officer or Contracting Officer's Representative, if authorized, during the term (term is defined as the period of performance for the basic contract and any options that may be exercised) of this contract. Technical Direction will provide specific information relating to the tasks contained in the Statement of Work and will be provided to the contractor in writing. Any Technical Direction issued hereunder will be subject to the terms and conditions of the contract. The contract shall take precedence if there is any conflict with any Technical Direction issued hereunder, and cannot be modified by any Technical Direction.

(b) As stated, Technical Direction shall be issued in writing and shall include, but not be limited to:

(1) date of issuance of Technical Direction;
(2) applicable contract number;
(3) technical direction identification number;
(4) description of Technical Direction;
(5) estimated cost;
(6) estimated level of effort by labor category; and
(7) signature of the PCO or COR.

(c) If the contractor does not agree with the estimated cost specified on the technical direction, or considers the technical direction to be outside the scope of the contract, it shall notify the PCO or COR immediately and, in the case of the estimated cost, arrive at a general agreement to the cost of the task. In the case of the direction requiring work that is out of the scope of the contract, the contractor shall not proceed with the effort unless and until the PCO executes a contract modification to include the change in scope.

## IX. POST-AWARD IDENTIFICATION AND ASSERTION OF RESTRICTIONS ON TECHNICAL DATA PERTAINING TO A COMMERCIAL ITEM AND COMMERCIAL COMPUTER SOFTWARE

a. Definitions. Unless otherwise specified in this provision, the terms used in this provision are defined in the FAR/DFARS, as applicable.

b. Post-award Assertions. In addition to the pre-award assertions made, other assertions on technical data pertaining to a commercial item and commercial computer software may be identified after award when based on new information or inadvertent omissions, unless the inadvertent omissions would have materially affected the source selection decision. Such identifications and assertions shall be submitted to the contracting officer as soon as practicable prior to the scheduled date for delivery of the technical data/computer software, using the table format found below and signed by an official authorized to contractually obligate the contractor.

| Commercial Technical Data/Computer Software Title, Version #, and License* | Technical Use/ Implementing Approach ** | If OSS, Was OSS modified by Contractor? *** | Name of Contractor Delivering Commercial Software**** |
|---|---|---|---|
| | | | |

* For commercial technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable

technical data and each such item, component, or process. For computer software or computer software documentation identify the computer software or computer software documentation. The complete title and version number of the computer software should be listed. If Open Source Software (OSS), the OSS license and version number should be listed. If a version number is not available, the contractor should state no version number. If commercial technical data is being delivered under the terms of DFARS 252.227-7015, then DFARS 252.227-7015 should be listed. If the OSS was downloaded from a website, the website address should also be provided. Enter none if all commercial technical data or commercial computer software will be submitted without restrictions.

** The functionality of the commercial computer software should be described, as well as where it is being used within the larger computer software deliverable (if applicable).

*** If OSS is being used, the contractor should state whether it has modified the OSS.

**** Corporation, individual, or other person as appropriate.

c. Licenses. The contractor shall provide copies of all commercial license(s) for the commercial technical data or commercial computer software that will be delivered. The Government will review the licenses to ensure that the license terms are consistent with federal procurement law and meet the Government's end user needs.

d. Use of OSS Without Delivery. The Government treats OSS as a category of commercial computer software. If the contractor proposes to use, but not deliver, commercial computer software (including OSS), the contractor must ensure that such use does not: (i) create, or purport to create, any Government distribution obligations with respect to the computer software deliverables; or (ii) grant, or purport to grant, to any third party any rights to or immunities under Government intellectual property or Government data rights to the Government computer software deliverables.

## X. CYBERSECURITY

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

**Cyber IT and Cybersecurity Personnel**

(a) The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

(b) The contractor shall be responsible for identifying, tracking and reporting cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Although the minimum frequency of reporting is monthly, the task order can require additional updates at any time.

(c) Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in para 8.2.2.4(b).

When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g., .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Pacific Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the NIWC Pacific IAM office. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.
2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the NIWC Pacific IAM office or from the website: https://navalforms.documentservices.dla.mil/.

(d) Contractor personnel with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

**Design, Integration, Configuration or Installation of Hardware and Software**

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum:

Acceptable Use of Department of the Navy Information Technology (IT) dated 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in para 5.2.2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

**Cybersecurity Workforce (CSWF) Report**

DoD 8570.01-M and DFARS PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report as applicable at the task order level. IAW DFARS clause 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided at the task order level, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

**Information Technology (IT) Services Requirements**

This paragraph only applies to IT contracts. Information Technology (IT) is defined as any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data of information by the agency. IT includes computers, ancillary equipment, peripherals, input, output, and storage devices necessary for security and surveillance. Electronic and Information technology (EIT) is IT that is used in the creation, conversion, or duplication of data or information. EIT includes: telecommunication products, such as telephones; information kiosks; transaction machines; World Wide Web sites; multimedia (including videotapes); and office equipment, such as copiers and fax machines.

**Information Technology (IT) General Requirements**

When applicable, the contractor shall be responsible for the following:

• Ensure that no production systems are operational on any RDT&E network.
• Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.
• Migrate all Navy Ashore production systems to the NMCI environment where available.
• Work with government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).
• Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.
• Register any contractor-owned or contractor-maintained IT systems utilized on contract in the Department of Defense IT Portfolio Registry (DITPR)-DON.
• Only perform work specified within the limitations of the task order.

**Acquisition of Commercial Software Products, hardware, and Related Services**

This paragraph only applies to the purchasing/hosting of commercial software. Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

**DON Enterprise Licensing Agreement/DOD Enterprise Software Initiative Program**

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dated 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and government-wide SmartBuy program (see DoD memo dated 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the task order level.

**DON Application and Database Management System**

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted